The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
05/10/2016

SUBJECT:
A Vulnerability in Adobe Flash Player Could Allow for Remote Code Execution (APSA16-02)

OVERVIEW:
A vulnerability has been discovered in Adobe Flash Player which could allow for remote code execution. Adobe Flash Player is a widely distributed multimedia and application player used to enhance the user experience when visiting web pages or reading email messages. Successful exploitation of this vulnerability may allow for remote code execution and allow an attacker to take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full system rights with failed exploit attempts will likely result in denial-of-service conditions.

THREAT INTELLIGENCE
Adobe is aware of a report that an exploit for CVE-2016-4117 exists in the wild.

SYSTEMS AFFECTED:
- Adobe Flash Player 21.0.0.226 and earlier for Windows, Macintosh, Linux, and Chrome OS

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:
An unspecified security vulnerability has been discovered in Adobe Flash Player which could allow for remote code execution.

Successful exploitation of this vulnerability may allow for remote code execution and allow an attacker to take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full system rights with failed exploit attempts will likely result in denial-of-service conditions.

RECOMMENDATIONS:

The following actions should be taken:

- Disable Flash functionality until a patch is released by Adobe.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources. Limit user account privileges to those required only.

REFERENCES:

Adobe:
https://helpx.adobe.com/security/products/flash-player/apsa16-02.html

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4117